УДК 327

П. П. Кирейчик, В. Д. Свирко,
курсанты 1-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Н. М. Канашевич,
профессор кафедры
социально-гуманитарных дисциплин
Могилевского института МВД,
кандидат исторических наук, профессор

КИБЕРВОЙНА В АРСЕНАЛЕ ГЛОБАЛИЗМА

Президент Республики Беларусь А. Г. Лукашенко неоднократно отмечал, что против Беларуси сегодня ведется «гибридная война», а вблизи наших границ уже создана сеть натовских киберцентров и развернуты кибервойска [1]. Термин «кибервойна» сегодня активно используется политиками, военными, журналистами, что требует его осмысления.

Прежде всего, отметим, что термин «кибервойна» в важнейших концептуальных документах белорусского государства рассматривается в непосредственной связи с понятиями «политика глобализма», «гибридная война» и «информационная война». Определим соотношение этих важнейших для понимания современных международных отношений и глобального развития понятий на основе анализа стратегических документов нашего государства, в которых рассматриваются новые угрозы и вызовы национальной безопасности.

Уже в Военной доктрине Республики Беларусь (2016) обращалось внимание на активизацию политиков ведущих западных стран, выступающих с позиций глобализма — совокупности идеологических, военных, культурных, пропагандистских идей, направленных на реализацию англосаксонского проекта либеральной глобализации планеты. Суть этого проекта можно свести к следующему: желательно повсеместное продвижение демократии, так как безопасность человека обеспечивается только при этом строе; возможно ограничение суверенитета извне для стран, затронутых внутренними конфликтами, включая гуманитарные интервенции.

Для сил глобализма сегодня характерно соединение классических и нетрадиционных инструментов политики не только открытых военных действий, провокаций, диверсий, но и таких новых форм насильственных действий, как гибридные войны и кибервойны.

В Военной доктрине Республики Беларусь был дан анализ гибридной войны — нетрадиционных видов действий, когда грани между войной и миром

стерты. Такие действия могут не иметь черты вооруженного конфликта, но в реальности представляют собой не что иное, как войну, хотя официально ее не объявляют. События в Ираке, Ливии, Сирии, Украине показывают, что конфликты по типу гибридных войн отличает вовлечение иррегулярных вооруженных формирований, привлечение наемных и гражданских лиц (повстанцев, сепаратистов, мятежников), организация протестных массовых беспорядков и поддержка их как извне, финансами и оружием, так и внутри страны — псевдорелигиозными и ультранационалистическими организациями, организованной преступностью.

Гибридные войны ведутся с масштабным использованием СМИ и киберпространства как для внутренней, так и для внешней аудитории. Важнейшими компонентами гибридных войн являются кампании по дискредитации правительств отдельных государств в форме масштабных и стремительных информационных и кибероперациий в сочетании с экономическим давлением.

В Концепции информационной безопасности Республики Беларусь отмечалось, что манипулирование массовым сознанием носит столь же острый характер, как и борьба за территории, ресурсы, рынки [2, с. 40]. Действия, которые обычно обозначают как информационные и кибервойны нередко на страницах популярных СМИ отождествляются. Однако в Концепции информационной безопасности Республики Беларусь эти кампании существенно различаются по объектам и средствам боевого воздействия.

Само понятие «информационная война» в данном концептуальном документе отсутствует, но используется понятие «деструктивное информационное воздействие», что понимается как негативное влияние на общественное сознание посредством дезинформации, PR-кампаний, других информационных операций с целью создания препятствий для нормального развития социально-экономических и политических процессов, функционирования государственных институтов и юридических лиц [2, с. 3].

Понятия же «кибератака», «киберинцидент», «кибертерроризм» в Концепции информационной безопасности рассматриваются в аспекте такого деструктивного воздействия на то или иное государство, когда оно осуществляется посредством программных или программно-аппаратных средств на объекты его информационной инфраструктуры и содержащуюся в них информацию [2, с. 4].

Таким образом, в современном мире информационный фактор, включая кибероперации, играет все более значительную роль в межгосударственных конфликтах, нередко принимающих характер «гибридной войны», а обеспечение безопасности информационного пространства и национальной информационной инфраструктуры — одно из условий сохранения и развития суверенного государства.

В этой связи считаем, что принципиальное значение для обеспечения национальной безопасности Беларуси имеет решение, принятое на VI Всебелорусском народном собрании, о модернизации информационной сферы и информационной политики, включая более широкое представление государственной позиции в Интернете, а также вовлечение в общие медийные проекты блогеров, лидеров общественного мнения, представителей общественных институтов.

В аспекте профессиональных интересов курсантов нашего учебного заведения особенно значима с учетом тенденции стремительного роста преступлений в информационной среде задача пресечения здесь экстремистской и мошеннической деятельности.

1. О единстве, развитии и независимости. Доклад Президента Александра Лукашенко на шестом Всебелорусском народном собрании 12 февраля 2021 г. [Электронный ресурс] // Беларусь сегодня. URL: https://www.sb.by/articles/lyubimuyu-ne-otdadim4.html (дата обращения: 02.06.2021). Перейти к источнику Вернуться к статье

2. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1. Доступ из справ.-правовой системы «Эталон». Вернуться к статье